



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

SOLDIER FITNESS TRACKER (SFT)

HQDA G3 - CSF2

### **SECTION 1: IS A PIA REQUIRED?**

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel\* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

\* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

## SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- New DoD Information System       New Electronic Collection
- Existing DoD Information System       Existing Electronic Collection
- Significantly Modified DoD Information System

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- Yes, DITPR      Enter DITPR System Identification Number
- Yes, SIPRNET      Enter SIPRNET Identification Number
- No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- Yes       No

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- Yes       No

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.  
Consult the Component Privacy Office for additional information or  
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office

Consult the Component Privacy Office for this date.

**e. Does this DoD information system or electronic collection have an OMB Control Number?**

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

**Yes**

**Enter OMB Control Number**

All PII is retrieved from other electronic data collection instruments

**Enter Expiration Date**

**No**

**f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.**

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 3013, Secretary of the Army; DoD Instruction 1100.13, Surveys of DoD Personnel; DoD Directive 6490.2, Comprehensive Health Surveillance; DoD Directive 6490.3, Deployment Health; DoD Directive 1404.10, Civilian Expeditionary Workforce; AR 600-63, The Army Health Program and E. O. 9397(SSN) as amended.

**g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.**

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The objective of SFT is to provide an information technology platform to support the Comprehensive Soldier and Family Fitness (CSF2) program. The web-based software application provides a comprehensive data collection and reporting capability designed to measure, track, and assess comprehensive fitness of all U.S. Army Soldiers (Active, Reserves and National Guard), beginning at recruitment, with reassessments at appropriate intervals continuing through transition or retirement. This capability also extends to Family members and DA Civilians. SFT operates the Global Assessment Tool (GAT), an online survey based instrument used to assess the dimensions of emotional, spiritual, social, and family fitness. SFT also makes self-development training available with Comprehensive Resilience Modules (CRMs). A management system tracks required and completed course work.

SFT collects personal, educational, military, and medical information.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The associated privacy risks with the PII collection are interception of transmitted data and unauthorized database access. Appropriate safeguards are in place for the collection and use of information, and we believe the risk to individuals' privacy to be minimal. The system operates in a secure facility. Information assurance and security awareness training is administered at in-processing and on an annual basis. Access to data is restricted to individuals authorized access to the system as stated in the governing Privacy Act system notice. The Common Access Card (CAC) login is enforced. Triple-DES level encryption is employed for data at rest. Hypertext Transfer Protocol Secure (HTTPS) is used with the Secure Sockets Layer (SSL) protocol for data in transit. Secure FTP (SFTP) is used for the transfer of data from other systems. SFT is an Installation Campus Network (ICAN) Tenant in Good Standing of the Army Analytics Group (AAG), its hosting environment. The environment is certified and accredited by the DoD Information Assurance Certification and Accreditation Process (DIACAP).

**h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.**

**Within the DoD Component.**

Specify.

Army agencies: Army Inspector General (IG); Assistant Secretary of the Army for Manpower and Reserve Affairs (ASA(M&RA)); Deputy Chief of Staff, G-1; Human Resources Command (HRC); Human Resources Command-St. Louis (HRC-St. Louis); Office of the Chief, Army Reserve (OCAR); Army General Counsel (GC); Secretary of the Army; US Army Reserve Command (USARC); Army Recruiting Command (USAREC); US Army Cadet Command; US Army Military Academy (USMA); Army Physical Disability Agency (PDA);

Other Army agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include Army Staff Principals in the chain of command, Department of Army Inspector General, Army Audit Agency, US Army Criminal Investigative Command, US Army Intelligence and Security Command, In addition, the Army blanket routine uses apply to this system.

**Other DoD Components.**

Specify.

**Other Federal Agencies.**

Specify.

**State and Local Agencies.**

Specify.

**Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

Yesmail Interactive is the service provider. Yesmail will measure the effectiveness of email delivery and manage the deliverability to ensure that no emails are marked as spam. The user's email address will be sent via an encrypted web service to the Yesmail platform. Yesmail is contractually obligated to treat the information as client confidential. As such its processes and access to the information is restricted and subject to the current PII laws. Yesmail is contractually obligated to delete the email address and content after emails have been sent.

**Other** (e.g., commercial providers, colleges).

Specify.

Yes mail Interactive, E-mail Service Provider (ESP)

**i. Do individuals have the opportunity to object to the collection of their PII?**

**Yes**

**No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

Individuals are not asked to enter any PII data nor does SFT modify the PII data. All data is received electronically from other Army information systems.

The Soldier implicitly consents to capture and use of PII at the time of employment or enlistment in the Armed Forces at which time they are provided a Privacy Advisory. Completion of the SFT GAT is a Command directed requirement ordered by the Army Chief of Staff. It is voluntary for the other user groups.

**j. Do individuals have the opportunity to consent to the specific uses of their PII?**

**Yes**

**No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

The Soldier implicitly consents to capture and use of PII at the time of employment or enlistment in the Armed Forces at which time they are provided a Privacy Advisory. Completion of the SFT GAT is a Command directed requirement ordered by the Army Chief of Staff. It is voluntary for the other user groups.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- |  |   |
|--|---|
| <input type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other                 | <input checked="" type="checkbox"/> None  |

Describe each applicable format.

SFT retrieved from existing PII data from other Army information systems itemized in Section 3, a, (2). Data is not collected directly from individual users.